

Are You Ready for **BY**



dy BYOD?

Advice from the trenches on how to prepare your wireless network for the bring-your-own-device movement.

By David Rath

W

HEN STUDENTS AND STAFF

returned to school in the **Jordan School District** (UT) after the 2011 Christmas break, Ron Bird could see that the number of devices on the wireless network had jumped by several hundred compared to pre-vacation levels. "I figured that was just whatever Mom and Dad bought kids for Christmas," says Bird, the district's network and technical services manager. "That's how fast the demand for access is growing."

Nevertheless, Bird and his colleagues felt like they were prepared. They already had spent several years building out their wired and wireless infrastructure, anticipating the emergence of the bring-your-own-device (BYOD) movement. "We knew the students were starting to bring their devices," Bird says, "and we would have to support that." Just over a year into BYOD, Jordan now supports approximately 2,000 students who bring their own devices to school.

Bird's experience in Jordan comes as no surprise to Philip Wegner, president of SecurEdge Networks in Charlotte, NC, which specializes in developing wireless networks for the K-12 sector. Wegner notes that just a few years ago he dealt almost exclusively with district-owned Windows-based PCs.

"Now it is much more heterogeneous, with iOS and Android devices," he says, "and, with the BYOD wave, even networks built in 2008 are starting to be outdated."

Many districts around the country face the same issues Jordan did as they launch their own BYOD initiatives. Putting aside the instructional questions, the infrastructure issues alone can be daunting.

T.H.E. Journal asked four K-12 technology leaders from all over the United States to describe the paths they took to BYOD, the preparations they made, the lessons they learned, and the most important questions they asked—or wish they'd asked.

Little by Little Hanover Public School District, Hanover, PA

Key to BYOD readiness: Years of gradual improvement to the wireless network

Top question to ask vendors: Can you segregate the BYOD traffic on the network?

When the school district in Hanover, PA, launched its BYOD program at 500-student **Hanover High School** last October, it already had several years of growth in its wireless infrastructure to build upon.

"We did have to make some adjustments to the wireless network for the BYOD project, but not as many as we had thought we would," says David Fry, the district's technology coordinator.

Hanover had started beefing up its wireless system in anticipation of moving to a 1-to-1 laptop program, but—as is the case in many districts—funding for an entire transition is not yet available, so a BYOD program became an incremental step. Five years ago, Hanover started with a much smaller iteration of wireless that had controls at individual access points. "But that proved unmanageable as we wanted to grow," Fry says. "We wanted a system with a central controller."

So, three years ago Hanover chose a system from Ruckus Wireless that added access points, but also the tools to adjust signals and do load balancing. "In many cases, that means dialing it down in cases where we have seven or eight access points overlapping," Fry says. (When laptops switch access points, it can sometimes cause dead periods that last as long as 10 seconds.)

"Ruckus also has tools that do a background scan and allow me to see any rogue access points," he explains. "Sometimes they are just in somebody's house near a school, but it does allow us to switch away from that channel."

Most consultants recommend placing BYOD traffic on a dedicated virtual network, separate from the district's own network, so there is no chance of those devices accessing budget or human resources data, which is the approach Fry took when he was building his network. "So now we have two different wireless networks," he says, "one for district equipment and one for personal electronic devices."

Using Ruckus' ZonePlanner, Hanover was able to handle that design process in-house. "We knew early on that we wanted

BEFORE YOU EVEN START...

When dealing with the technical and security issues associated with launching a BYOD program, one of the first decisions has to be whether you are going to outsource the function, seek consulting help, or make it a do-it-yourself project. Do you have the expertise on staff to design and manage the expansion of a wireless network?

Even if the answer is yes to that question, can you handle what is sure to be a dynamic, growth-focused situation in the future? Keep in mind something the IT consulting firm Gartner has estimated: 80 percent of newly installed wireless networks will be obsolete by 2015 due to improper or insufficient planning.

Philip Wegner, president of SecurEdge Networks in Charlotte, NC, details some of the specific network infrastructure requirements that any districts considering a new BYOD initiative should take into account before they begin their work:

- **Capacity vs. coverage.** Wegner suggests district technology leaders think about the capacity of the proposed network, not just coverage of areas. If an auditorium has just one access point, it could quickly get overloaded. "You have to have the density of coverage to support users and be able to plan ahead and design for that," he says.
- **Directory services and device registration.** You'll need a database of the user groups and the devices registered to each user, Wegner says. The credentials created for each person in your directory service should also be used to authenticate the user on the wireless infrastructure so that you have one database of users accessing the network.
- **Role-based access control.** You'll want to segment user groups based on role, and limit what they can access. Your system must have directory services integration and be able to assign roles to users. "For instance," Wegner says, "students might be limited to using the network to access the internet and their own files," while faculty and staff might be able to do more than that.
- **Application-level filtering.** The latest generation of firewalls has application-level filtering and control. That is, they know which applications students are using and which sites they are trying to access, Wegner says. That allows network administrators to write specific policies about how much bandwidth each student can use when accessing YouTube, for instance. Wegner also suggests having network traffic flow through a device that checks for viruses or malicious activity.

There are many wireless vendors to choose from, adds David Soper, president of netDirective Technologies in Melbourne, FL. But conducting a needs analysis and understanding compliance requirements up front will help you narrow down product choices. As an example, he points out, "One mistake we see some schools make is starting out buying consumer-grade access points with no form of centralized management. They just buy off-the-shelf products and hope for the best. But without a centralized controller, there is no way to see what is happening on the network or to detect rogue access points."

to do that," Fry says, "and the Ruckus design tools made it pretty easy."

One limitation is that there currently is no printing option from a personally owned device. This might change as the district updates the way the school's printers are configured. Until then, students have the option of accessing their document from a school computer when they want to print something.

No More Wild West Jordan School District, UT

Key to BYOD readiness: Made good use of vendor site survey and network design tools to compute bandwidth and throughput estimates, which helped determine the best places to put access points

Top question to ask vendors: Does your solution offer spectrum analysis so we can see what is happening on the network and make adjustments?

A few years ago, Utah's Jordan School District was the Wild West when it came to wireless network infrastructure. Each school in the district, which serves more than 50,000 students in the communities of Bluffdale, Copperton, Herriman, Riverton, South Jordan, and West Jordan, did its own thing about wireless access. They used a hodgepodge of different equipment and, of course, ran into radio frequency interference. One group of teachers, with the best of intentions, bought 10 Linksys access points but, because they didn't understand the settings, were never able to route them anywhere.

"We used examples like that to make the case for an enterprise wireless network districtwide," recalls Bird. "We looked at other vendor options but decided to go with 3Com, largely because we already used their switches and phone equipment. After an investigation, it seemed like the simplest thing to do." (HP has since acquired 3Com.)

Jordan's network has grown rapidly to 310 sensors for 1,300 access points, a

little more than four per sensor. The district now has 2,000 students

who bring their own devices, with another 5,000 school-assigned devices on the wireless network and about 15,000 on the wired network.

How did Bird know he would have enough access points in the right places to provide good performance for so many devices? He and his staff got floor plans for all the buildings, including information about where all the brick walls were, from the facilities maintenance team, he says. The 3Com network design tool pulls all that information in, computes bandwidth and throughput estimates, and then tells you the optimal places for your access points. "There was no way for us to know whether it was going to be accurate or not," Bird says. "We just had to cross our fingers. But we have actually been very pleased with it."

With a site survey tool within Fluke Networks' AirMagnet product, Bird can stroll the campuses and measure signal strength. "We do get complaints about performance at times from students or teachers," he says. "Usually it is not the network itself, but something like a wireless microphone or camera causing interference."

Previously, a wireless audiovisual system might have caused interference with a network. Bird's team would get a call from a middle school, for instance, and by the time they got there, the device would be off and put away and the network would be working fine. "It was frustrating," he says. "We couldn't pinpoint the problem without these tools."

With the spectrum analyzer, sensors track wireless access points, then the system triangulates where the interference is coming from.

Love Your Network Park Hill School District, Kansas City, MO

Key to BYOD readiness: Upgrading to 802.11n technology

**[keyword: byod
visit thejournal.com]**

Top question to ask vendors: Can you demonstrate flexibility and agility in the wake of changing needs?

In the fall of 2011, **Park Hill School District** in Kansas City, MO, piloted BYOD with a segment of the student population and staff. As he planned to open it up to everyone else at the district's two high schools this spring, Brad Sandt, Park Hill's director of technology, says the growth of the enterprise wireless network has been an evolutionary process, but the biggest change was the upgrade to 802.11n.

"The technology enhancements with the 802.11n standard over the a/b/g standard have been noticeable," Sandt says. "We have had few signal-connection issues, and the speeds are significantly higher." (The access points have the potential for 600-Mbps speeds.)

The upgrade of the core switching network and wireless network cost approximately \$1.3 million, which covered switches in 19 facilities and 750 access points. One of the high schools now has about 200 BYOD devices that are regularly on the network; district staff members have registered more than 300 additional devices to date on a separate staff BYOD network.

Park Hill has always used Cisco Systems equipment, so Sandt believed it made sense to stay with Cisco for this evolution. The district uses M86 Security for its web filtering and reporting functions. "We leverage a RADIUS server for authentication, authorization, and MAC filtering to register the device, so that process is seamless to the students on their iPads," he says. "They sign on to the network just as your device would if you were staying at a hotel."

"The challenge we missed early on was how much love you have to give the network," Sandt says. "We learned it requires constant attention, nearly on a daily basis. Access points may fail. It may require more resources than you originally think. It's possible that you could outsource the management function at some point but, when we have looked at that in the past, we

haven't found anyone with the expertise we are looking for."

Park Hill went to the reseller and consulting firm CDW-G for advice on best practices and potential future technologies. "They have played a critical role in helping us plan for and anticipate changing network environments," Sandt says. "We continue to enhance, troubleshoot, and modify our network based on changing demands, environmental conditions, and experience. I would strongly suggest that districts planning on wireless deployments view them as continual projects, instead of a one-time project."

With that in mind, Sandt says, the most important thing to ask vendors about is flexibility and agility: Is it a system you can keep building onto as the number of users on the network grows? He says consultants told him that systems from companies such as Aruba Networks, Cisco, and Aerohive Networks are designed to add capacity easily. But other vendors in your ecosystem should be flexible as well, Sandt stresses. "What happens if I need a new level of security?" he asks.

Partners for Life

Holy Trinity Episcopal Academy, Melbourne, FL

Key to BYOD readiness: Contract out to a wireless network management team that can continually fine-tune the WLAN to improve performance.

Top question to ask vendors: How does your solution deal with our specific building parameters?

As the 840-student PreK-12 **Holy Trinity Episcopal Academy** in Melbourne, FL, prepared to pilot BYOD last year, Susan Bearden, the school's director of information technology, realized the most important decision she made was selecting the right service provider.

Holy Trinity began the pilot with its 11th- and 12th-graders, Bearden says. It now has about 300 students bringing their

own devices to school. The BYOD effort required a number of changes to the wireless network infrastructure at Holy Trinity. Frank Huston, vice president of netDirective, its service provider, remembers an early conversation with Bearden.

"We knew this [BYOD] train was coming," he says. "The question was, 'Are we going to get on it or get run over by it?' We had to address content filtering, and we had to take into account the possibility of growth. The coverage had to be scalable, and we had to make sure the access points wouldn't get overloaded."

Holy Trinity has separate campuses for its upper and lower grades, each with its own wireless network and its own controller. The upper school already had a system that had been installed by Meru Networks before netDirective got involved. Because there is less demand in the lower school, netDirective decided the relatively sophisticated Meru system would be "overkill" and instead installed HP ProCurve, which Huston described as a simpler, more economical solution. The plan is to eventually have one vendor's system that will be in place across both schools.


"We began partnering with netDirective Technologies in 2009, in part because we are able to take advantage of their skill set in network design and administration," Bearden says. "They have experience working with multiple companies and, in this particular area of IT, that is expertise we are willing to pay for." (NetDirective is in the process of merging with Artemis International Technologies.)

Huston suggests interviewing at least three wireless network vendors in depth to get a true evaluation of whether they can address a specific customer's needs. "I talked to the engineers and the sales team to explain what we needed and I had to get an understanding that they have worked in a K-12 environment. This school has areas with concrete structures, and density is a big issue. You have to ask vendors how their solution fits into that space. If they are not asking you for your floor plans, that

is a red flag."

Bearden says she has grown to appreciate the fact that a wireless network is not something you simply purchase, set up, and then leave alone. It requires continual adjustments based on usage growth.

Often usage will shift as a room is rearranged or put to new uses, Huston notes. The netDirective executives are fans of high-gain antennas to boost signal strength, especially on large campuses. "You have spikes in usage you have to deal with, and it is never a static solution," Huston says.

Bearden says BYOD has been a huge student and parent satisfier so far but, she adds, if you are going to make the investment, you have to make sure it is working consistently. "If there are bumps in the road, you have to address them quickly," she says, "and take them seriously because now you are disrupting what they are doing in the classroom." 

David Rath is a freelance technology writer based in Philadelphia.

LINKS

- **Aerohive Networks**
aerohive.com
- **Aruba Networks**
arubanetworks.com
- **CDW-G**
cdwg.com
- **Cisco Systems**
cisco.com
- **Fluke Networks**
flukenetworks.com
- **HP**
hp.com
- **M86 Security**
m86security.com
- **Meru Networks**
merunetworks.com
- **netDirective Technologies**
netdirectivetechologies.com
- **Ruckus Wireless**
ruckuswireless.com

Copyright of T H E Journal is the property of T.H.E. Journal and its content may not be copied or emailed to multiple sites or posted to a listserv without the copyright holder's express written permission. However, users may print, download, or email articles for individual use.